NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 105522A/105832A
11 March 2019

RAMYA KRISHNAN
ADI KAMDAR
KNIGHT FIRST AMENDMENT INSTITUTE
AT COLUMBIA UNIVERSITY
475 RIVERSIDE DRIVE SUITE 202
NEW YORK, NY 10115

AVI ASHER-SCHAPIRO
COMMITTEE TO PROTECT JOURNALISTS
330 7th AVE, 11th FLOOR
NEW YORK, NY 10001

Dear Ms. Krishnan and Mr. Schapiro:

This letter accompanies NSA's final response to the 19 October 2018 Freedom of Information Act (FOIA) request on behalf of the Knight First Amendment Institute, and the 20 November 2018 FOIA request on behalf of the Committee to Protect Journalists for the following:

1. All procedures or guidance for determining whether to warn, or for delivering a warning to, an intended victim or those responsible for protecting the intended victim, pursuant to Directive 191;

2. All records concerning the duty to warn under Directive 191 as it relates to Jamal Khashoggi, including any records relating to duty to warn actions with respect to him;

3. All records concerning any 'issue aris[ing] among IC elements' regarding a determination to warn Jamal Khashoggi or waive the duty to warn requirement, or regarding the method for communicating threat information to him.

The request on behalf of the Knight First Amendment Institute was assigned FOIA Case Number 105522, and the request on behalf of the Committee to Protect Journalists was assigned FOIA Case Number 105832. On 20 November 2018, the Knight First Amendment Institute filed a complaint which included NSA, initiating the litigation regarding the above-described FOIA requests. Your cases have been processed in accordance with FOIA.

Item 1

Two documents (21 pages) responsive to item 1 are enclosed: (1) *NSA/CSS Policy Instruction 2-0003 (Duty to Warn)* and (2) *Duty to Warn Operating Procedures.*[1] Certain information has been deleted from the enclosures, as explained below.

Some of the information deleted from the documents was found to be currently and properly classified in accordance with Executive Order 13526. This information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified SECRET as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause serious damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. § 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA (5 U.S.C. § 552(b)(3)), which provides for the withholding of information specifically protected from disclosure by statute. The statute applicable in this case is Section 6, Public Law 86-36 (50 U.S.C. § 3605).

Items 2 and 3

Regarding items 2 and 3 of your requests, we have determined that the fact of the existence or non-existence of the materials you request is a currently and properly classified matter in accordance with Executive Order 13526, as set forth in Subparagraph (c) of Section 1.4. Thus, we can neither confirm nor deny the existence of responsive records, pursuant to the first exemption of the FOIA (5 U.S.C. § 552(b)(1)), which provides that the FOIA does not apply to matters that are specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign relations and are, in fact, properly classified pursuant to such Executive Order.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. The third exemption of the FOIA provides for the withholding of information specifically protected from disclosure by statute. Thus, the existence or non-existence of the information is also exempted from disclosure pursuant to the third exemption. The specific statutes applicable in this case are 18 U.S.C § 798; 50 U.S.C § 3024(i); and Section 6, Public Law 86-36 (50 U.S.C. § 3605).

NSA collects and provides intelligence derived from foreign communications to policymakers, military commanders, and law enforcement officials. We do this to help these individuals protect the security of the United States, its allies, and their citizens from threats such as terrorism, weapons of mass destruction, foreign espionage, international organized crime, and other hostile activities. What we are authorized to do, and how we do it, is described in Executive Order 12333. Information about how

---

[1] Please note that the policy instruction cited in *Duty to Warn Operating Procedures, NSA/CSS Policy Instruction 11-0002 (Duty to Warn),* is an unpublished version of 2-0003. 11-0002 was the numbering given to 2-0003 prior to publication.

NSA conducts signals intelligence activities is available on the websites of NSA (www.nsa.gov) and the Office of the Director of National Intelligence (www.dni.gov).

Please be advised that NSA has completed its processing of your cases.

Sincerely,

for Shawn C. Lukas

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY INSTRUCTION
2-0003

Issue Date: 20 May 2018
Revised:

(U) DUTY TO WARN

(U) PURPOSE AND SCOPE

(U) This policy instruction implements Intelligence Community Directive (ICD) 191, "Duty to Warn" (Reference a), and supplements United States Signals Intelligence (SIGINT) Directive (USSID) CR1252, "Reporting of Threat Warning Information" (Reference b). It establishes procedures for providing warning regarding threats of *intentional killing*, *serious bodily injury*, and *kidnapping* to specific individuals or groups.

(U) This policy instruction applies to *NSA/CSS employees*.

(U) This policy instruction is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States; its departments, other agencies, or entities; its officers, employees, or agents; or any other person.

PAUL M. NAKASONE
General, U.S. Army
Director, NSA/Chief, CSS

[redacted]

Endorsed by
Chief, Policy

(b)(3)-P.L. 86-36

(U) Encls:
Annex A – Duty to Warn Procedures
Annex B – Dispute Resolution Procedures
Annex C – Duty to Warn Procedures for Second Party Reports and NSA/CSS Reports from Second Party Collection
Annex D – Contact Information

(U) DISTRIBUTION:
K1M
P12
P134 (Vital Records)

(U//~~FOUO~~) This policy instruction supersedes National Security Agency CR-679-01, "Terrorist Threat Advisories-Reporting Threat to Civilian Entities," dated 3 December 2007.
(U) OPI: National Security Operations Center (NSOC), K1, 963-3777s.
(U) No section of this document shall be released without approval from the Office of Policy (P12).

(U) POLICY

1. (U) Any NSA/CSS element that collects or acquires credible and specific information indicating an impending threat of intentional killing, serious bodily injury, or kidnapping directed at a person or group of people (hereafter referred to as "intended victim") shall have a *duty to warn* the intended victim or those responsible for protecting the intended victim, as appropriate (Reference a). This includes threats where the target is an institution, place of business, structure, location, or electronic infrastructure that supports life. The term "intended victim" includes both U.S. persons, as defined in Executive Order 12333, "United States Intelligence Activities" (Reference c), and non-U.S. persons.

2. (U) NSA/CSS shall execute its duty to warn in accordance with the Duty to Warn Procedures in Annex A, rather than through the Terrorist Threat Advisory procedures outlined in Reference b. The procedures for sharing Threat Warning Tippers, also outlined in Reference b, shall remain the same.

3. (U//~~FOUO~~) Duty to warn may be waived if any of the following waiver justifications apply:

a. (U//~~FOUO~~) The intended victim, or those responsible for ensuring the intended victim's safety, is/are already aware of the specific threat;

b. (U//~~FOUO~~) The intended victim is at risk only as a result of the intended victim's participation in an insurgency, insurrection, or other armed conflict;

c. (U//~~FOUO~~) There is a reasonable basis for believing that the intended victim is a terrorist, a direct supporter of terrorists, an assassin, a drug trafficker, or involved in violent crimes;

d. (U//~~FOUO~~) Any attempt to warn the intended victim would unduly endanger U.S. Government personnel, sources, methods, intelligence operations, or defense operations;

e. (U//~~FOUO~~) The information resulting in the duty to warn determination was acquired from a foreign government with whom the U.S. has formal agreements or liaison relationships, and any attempt to warn the intended victim would unduly endanger the personnel, sources, methods, intelligence operations, or defense operations of that foreign government; or

f. (U) There is no reasonable way to warn the intended victim.

4. (U//~~FOUO~~) Issues concerning whether threat information is credible and specific, so as to permit a meaningful warning, shall be resolved in favor of informing the intended victim if none of the waiver justifications above are present.

5. (U//~~FOUO~~) If issues arise among NSA/CSS organizations or between NSA/CSS and Intelligence Community (IC) elements regarding a determination to warn an intended victim or waive the duty to warn requirement, the methods of communicating the threat information to the intended victim, or the timely receipt of related feedback from the receiving customer offices, resolution shall occur at the lowest practical and authorized level in a manner that does not unnecessarily delay the timely notification of threat information to the intended victim.

6. (U) If an issue in dispute between the IC elements has been elevated to the Director, NSA/Chief, CSS (DIRNSA/CHCSS) and attempts at resolution remain at an impasse, the DIRNSA/CHCSS shall notify the Director of National Intelligence (DNI). The DNI will facilitate resolution of the issues that have been referred.

(U) PROCEDURES

7. (U//~~FOUO~~) Annex A contains NSA/CSS' duty to warn procedures, which are consistent with Reference a.

(U) RESPONSIBILITIES

8. (U) The Director, NSA/Chief, CSS (DIRNSA/CHCSS) shall:

a. (U//~~FOUO~~) Provide information to the DNI, upon request, regarding NSA/CSS' duty to warn procedures and actions; and

b. (U) Notify the DNI when an issue in dispute among the IC elements requires the DNI's resolution.

9. (U//~~FOUO~~) The Director, Operations (X) shall serve as the final adjudicator for internal NSA/CSS disputes regarding duty to warn during normal business hours when such disputes cannot be resolved at a lower level.

10. (U) The Director, National Security Operations Center (NSOC) shall:

a. (U//~~FOUO~~) Manage the duty to warn process at NSA/CSS; and

b. (U//~~FOUO~~) Maintain records on duty to warn determinations, including decisions to waive the requirement and any actions taken to warn the intended victim (Reference a).

11. (U//~~FOUO~~) The NSOC Senior Operations Officer (SOO) shall serve as the final adjudicator for internal NSA/CSS disputes regarding duty to warn after normal business hours when such disputes cannot be resolved at a lower level.

12. (U//~~FOUO~~) The NSOC Senior Reporting Officer (SRO) shall manage duty to warn post-publication requests after normal business hours.

13. (U//~~FOUO~~) The Chief, Information Sharing and Collaboration [redacted] shall manage duty to warn post-publication requests during normal business hours.

14. (U//~~FOUO~~) Office-level (i.e., Alpha +2) management or operations staff shall approve duty to warn waiver requests.

15. (U//~~FOUO~~) The Branch Chief, Section Chief, Division Chief, Operations Officer, or Chief of Operations in the appropriate target office shall affirm whether threat information is credible and specific, so as to permit meaningful warning.

(b)(3)-P.L. 86-36

16. (U) NSA/CSS employees shall:

a. (U) Identify credible and specific information indicating an impending threat of intentional killing, serious bodily injury, or kidnapping of an individual or group and shall immediately report this information to their management for a determination on whether to warn the intended victim; and

b. (U//~~FOUO~~) Submit duty to warn waiver requests, if any of the waiver justifications apply (see paragraph 3), to Office-level management or operations staff.

(U) REFERENCES

17. (U) References:

a. (U) Intelligence Community Directive (ICD) 191, "Duty to Warn," dated 21 July 2015.

b. (U//~~FOUO~~) USSID CR 1252, "Reporting of Threat Warning Information," dated 26 November 2007, revised 18 February 2010.

c. (U) Executive Order 12333, "United States Intelligence Activities," as amended.

(U) DEFINITIONS

18. (U) Duty to Warn – A requirement to warn U.S. and non-U.S. persons of impending threats of intentional killing, serious bodily injury, or kidnapping (Reference a).

19. (U) Intentional Killing – The deliberate killing of a specific individual or group of individuals (Reference a).

20. (U) Kidnapping – The intentional taking of an individual or group through force or threat of force (Reference a).

21. (U) NSA/CSS Employee – A person employed by, assigned or detailed to, or acting for an element within NSA/CSS (derived from Reference c).

22. (U) Serious Bodily Injury – An injury that creates a substantial risk of death or causes serious, permanent disfigurement or impairment (Reference a).

(U) ANNEX A

(U) DUTY TO WARN PROCEDURES

1. (U) The NSA/CSS employee identifies or is informed of credible and specific information indicating an impending threat of intentional killing, serious bodily injury, or kidnapping of an individual or group.

2. (U//~~FOUO~~) The NSA/CSS employee immediately reports the information to a manager (i.e., their Branch Chief, Section Chief, Division Chief, Operations Officer, or Group Chief).

3. (U) The NSA/CSS employee's manager consults with the Target Office Chief (or the Target Office Chief's designee) and determines whether the threat information is credible and specific, so as to permit a meaningful warning.

4. (U//~~FOUO~~) If the NSA/CSS employee's manager determines that the threat information is credible and specific, the employee assesses whether any of the waiver justifications apply. If any apply, the NSA/CSS employee requests a waiver from their Office-level (i.e., Alpha +2) management or operations staff:

a. (U//~~FOUO~~) The waiver requester sends the appropriate justification, brief description of the threat, and information on which the threat is based with a link to or copy of the report in which the threat is documented.

b. (U//~~FOUO~~) The Office-level reviewer responds by approving or denying the waiver request. If they approve the waiver, then they include the NSOC threat warning alias [redacted] to document the response with NSOC.

5. (U//~~FOUO~~) If none of the waiver justifications apply or the waiver request is denied, the NSA/CSS employee informs the element that will issue the warning that a duty to warn notification is in progress:

a. (U) If the intended victim is located in the United States, the NSA/CSS employee or their manager informs the Federal Bureau of Investigation (FBI), through the NSA/CSS Representative (NCR) FBI if appropriate. (See Annex D for FBI contact information.)

b. (U) If the intended victim is located outside of the United States, the NSA/CSS employee or their manager informs the DNI Representative/Chief of Station (DNIR/COS), through the Cryptologic Services Group (CSG) Central Intelligence Agency (CIA), and, if appropriate, [redacted] (See Annex D for CIA contact information.)

[redacted] (b)(3)-P.L. 86-36

6. (U//~~FOUO~~) The NSA/CSS employee submits a pro-active post-publication release request against the report containing the threat information, whereby the NSA/CSS employee shall:

a. (U//~~FOUO~~) Go to [redacted]

b. (U//~~FOUO~~) Select the appropriate task type from the menu based on the classification of the original report, the end recipient, and inclusion of unmasked identities.

c. (U) Complete the form providing the following information:

(b)(3)-P.L. 86-36

1) (U//~~FOUO~~) **Email Address** – At minimum, the NSA/CSS employee shall include their email address or office alias; their office's operations team alias, post-pub team alias, and NSOC desk alias; and the NSOC SRO [redacted] and appropriate NSA/CSS liaison element [redacted] and [redacted]

2) (U//~~FOUO~~) **Justification** – Detail the purpose for sharing this information with the intended recipient. (For example: "[Appropriate Classification] This is a pro-active Duty to Warn (DTW) release to [Name of Potential Victim/s] based on [Report Serial Number]. We believe that [Name of Potential Victim/s] is in imminent danger. We request that this information be relayed to the intended recipient as soon as possible to allow them time to take appropriate precautions.")

3) (U//~~FOUO~~) **Handling Precedence** – If the threat is imminent, submit the request with URGENT precedence. If the threat is not imminent, submit the request with Immediate or Priority precedence.

4) (U//~~FOUO~~) **Release Classification** – The classification of requests varies, but is often UNCLASSIFIED. The most appropriate classification should allow the intended recipient to receive the warning at the chosen classification, but is not unnecessarily sanitized if the recipient is authorized for SECRET or TS//SI reporting.

5) (U) **Proposed Sanitization** – Use the below format in the Proposed Sanitization text field:

Please pass this to CIA (if threat is outside of U.S.) or FBI (if threat is in U.S) with the text to be released:

[Appropriate Classification] This is a pro-active Duty to Warn (DTW) release to [Name of Potential Victim/s] based on [Report Serial Number]. We believe that [Name of Potential Victim/s] is in imminent danger. We request that this information be relayed to the intended recipient as soon as possible to allow them time to take appropriate precautions.

(U//~~FOUO~~) Per ICD 191, NSA is required to document and maintain records on specified duty to warn actions, one of them being how and when threat information was delivered to the intended victim. We kindly request notification of your Agency's actions within 5 business days from the date of notification for this purpose.

==========

Text to Be Released:
[Appropriate Classification] [Warning language goes here.] (*If the language is UNCLASSIFIED, it must be approved by Office-level Chief of Operations, Deputy Chief of Operations, Chief, or Deputy Chief.)

==========

a) (U//~~FOUO~~) If the post-publication request is marked Immediate and submitted during normal business hours, [redacted] assigns the request through standard post-publication procedures and includes the NSOC Threat Warning alias [redacted] on all duty to warn email communications.

(b)(3)-P.L. 86-36

b) (U//~~FOUO~~) If the post-publication request is marked Immediate and submitted after normal business hours, the NSOC SRO processes the request. NSOC should reach out to the appropriate target office designee for advice or concurrence before any release after normal business hours.

7. (U//~~FOUO~~) The post-publication request is formally reviewed in accordance with standard post-publication processes, which include Collection, Exploitation, and Cryptanalysis Operations [redacted] Second Party; and Third Party reviews, as appropriate.

8. (U//~~FOUO~~) [redacted] or the NSOC SRO provides the approved release language to the customer, who is responsible for providing the warning. [redacted] or the NSOC SRO informs the customer that once the approved language is released, the customer has 5 business days to provide feedback on language use.

(U) ANNEX B

(U) DISPUTE RESOLUTION PROCEDURES

1. (U//~~FOUO~~) Any internal disputes among NSA/CSS employees or organizations should be resolved at the lowest practical and authorized level. The Director of Operations shall be the final adjudicator for internal NSA/CSS disputes during normal business hours; the NSOC SOO shall be the final adjudicator after normal business hours.

2. (U//~~FOUO~~) When an NSA/CSS customer disputes a duty to warn waiver determination, the customer may request that NSA/CSS reconsider:

a. (U) During normal business hours:

(b)(3)-P.L. 86-36

1) (U//~~FOUO~~) The Chief, [redacted] or Chief, [redacted] reviews the request to reconsider and consults with the NSOC SOO.

2) (U) The Chief [redacted] or Chief [redacted] decides whether to uphold the duty to warn waiver determination.

b. (U) After normal business hours:

1) (U//~~FOUO~~) The NSOC SOO reviews the request to reconsider and consults with the appropriate operations desks on the NSOC floor.

2) (U) The NSOC SOO decides whether to uphold the duty to warn waiver determination.

3. (U//~~FOUO~~) If an NSA/CSS employee has not received feedback from an NSA/CSS customer on the uses of its released duty to warn language and has made reasonable and documented steps to receive feedback, the NSA/CSS affiliate may contact the appropriate NSA/CSS liaison office (NCR FBI or CSG CIA) to facilitate resolution. (See Annex D for NCR FBI and CSG CIA contact information.)

4. (U//~~FOUO~~) When an NSA/CSS employee disputes a customer's decision to deliver threat information to an intended victim in an expeditious manner without prior consultation or notification, the NSA/CSS employee may contact the appropriate NSA/CSS liaison office (i.e., NCR FBI or CSG CIA) to facilitate resolution.

(U) ANNEX C

(U) DUTY TO WARN PROCEDURES FOR SECOND PARTY REPORTS AND NSA/CSS REPORTS FROM SECOND PARTY COLLECTION

1. (U//~~FOUO~~) The Chief, [redacted] or the NSOC SRO informs the appropriate Special United States Liaison Office (SUSLO) as soon as duty to warn threat information is identified.

2. (U//~~FOUO~~) The SUSLO coordinates with the DNIR/COS/Regional Security Officer to ensure duty to warn requirements are met. The SUSLO should engage with the partner according to established sharing guidelines. (See SUSLO contact information in Annex D.) Contact NSOC for afterhours support.

[redacted] (b)(3)-P.L. 86-36

(U) ANNEX D

(U) CONTACT INFORMATION

(U//~~FOUO~~) **FBI CT Watch**:
534-1463
[redacted]

(U//~~FOUO~~) **FBI Strategic Information and Operations Center**:
534-1463
[redacted]

(U//~~FOUO~~) **NCR FBI**:
[redacted]
717-7116 or 931-6966 (secure)
[redacted]
NCR FBI Personnel Roster

(U//~~FOUO~~) **CSG CIA**:
[redacted]
935-0209 (secure)
[redacted]

(U//~~FOUO~~) [redacted]

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **NSOC Senior Operations Officer (SOO)**:
[redacted]
963-3777 (secure)
[redacted]

(U//~~FOUO~~) **NSOC Directorate of Operations, Operations Management (DOOM)**:
[redacted]
963-3069 (secure)
[redacted]

(U//~~FOUO~~) **NSOC Counterterrorism Operations Cell Senior Leader (CT-LDR)**:
[redacted]
966-6073 (secure)

(U//~~FOUO~~) **NSOC Senior Reporting Officer (SRO)**:
[redacted]
963-3278 (secure)

(U//~~FOUO~~) **SUSLO-London**:
995-7201 (secure)
[redacted]

(U//~~FOUO~~) **SUSLO-Canberra**:
263-2100 (secure)

(U//~~FOUO~~) **SUSLO-Ottawa**:
262-2034 (secure)
[redacted]

(U//~~FOUO~~) **SUSLO-Wellington**:
717-8639/8638 (secure)

[redacted] (b)(3)-P.L. 86-36

(U) DUTY TO WARN STANDARD OPERATING PROCEDURES JULY 2017

(U) This document provides procedures for United States SIGINT System (USSS) elements in meeting duty-to-warn responsibilities IAW Intelligence Community Directive (ICD) 191, *Duty to Warn*. The procedures established in this document are intended to supplement those outlined in NSA Policy Instruction 11-0002, *Duty To Warn*.

Policy

(U//~~FOUO~~) What is a threat?

- (U) USSS elements that collect or acquire ***credible*** and ***specific*** information indicating an ***impending*** threat of intentional killing, kidnapping, or serious bodily injury directed at a person or group of people (hereafter referred to as intended victim) have a duty to warn the intended victim.[1] This includes threats where the target is an institution, place of business, structure, location, or electronic infrastructure that supports life. Intended victims include both U.S. persons, as defined in Executive Order 12333, "United States Intelligence Activities," and non-U.S. persons.

(U//~~FOUO~~) What can be waived?

- (U) ICD 191 includes provisions whereby NSA can determine under what circumstances the duty to warn requirement may be waived. The following are examples of appropriate waiver justifications, although this is not an inclusive list:
    - (U) The intended victim, or those responsible for ensuring the intended victim's safety, is already aware of the specific threat;
    - (U) The intended victim is at risk only as a result of the intended victim's participation in an insurgency, insurrection, or other armed conflict;[2]

(b)(3)-P.L. 86-36

[1] (U//~~FOUO~~) Duty to warn, in accordance with ICD 191 and NSA Policy 11-0002, does not apply to cyber-related threats in the strict sense that cyber-related tactics, techniques, and procedures do not directly pose the threat of physical harm to an individual. USSS elements that identify cyber incidents that could indirectly result in threat to life (e.g. indications of crippling networks supporting transportation or communications via cyber means) should consult NSA/CSS cyber-related blanket dissemination authorities and guidance on the Dissemination Guidance and Production Services [redacted] web page ('go reporting').

[2] (U//~~FOUO~~) The Director of Policy for the Office of the Director of National Intelligence has stated that ICD 191 is not intended to pose a burdensome requirement of providing a waiver for each individual scenario in an armed conflict, such as in Iraq where terrorists and armed forces are engaged. NSA should reduce the documentation requirements for waivers when the threat activity consists of an ongoing conflict between terrorist and other armed combatants. With this in mind, documentation of a Duty to Warn waiver request is not required in situations when the threat is against U.S. declared Foreign Terrorist Organizations or persons/elements participating in an armed conflict unless civilians or non-participants in these organizations/actions are at risk.

- (U) There is a reasonable basis for believing that the intended victim is a terrorist, a direct supporter of terrorists, an assassin, a drug trafficker, or involved in violent crimes;
- ~~(S//NF)~~ Signals intelligence activities undertaken in support of military operations
- (U) Any attempt to warn the intended victim would unduly endanger U.S. Government personnel, sources, methods, intelligence operations, or defense operations;
- (U//~~FOUO~~) The information resulting in the duty to warn determination was acquired from a foreign government with whom the U.S. has formal agreements or liaison relationships, and any attempt to warn the intended victim would unduly endanger the personnel, sources, methods, intelligence operations, or defense operations of that foreign government; or
- (U) There is no reasonable way to warn the intended victim.

Process

(U) Identify Threat

- (U//~~FOUO~~) The USSS analyst, management, operations officers, or the National Security Operations Center (NSOC) identifies or is informed of possible duty-to-warn information.[3, 4]
- (U//~~FOUO~~) The possible threat is raised to designated target office POC (typically Division or Office-level Operations Officer or Chief of Operations).

(U) Assess Threat

- (U//~~FOUO~~) The analyst/management/operations staff assess the threat to determine if the threat is specific, credible, and impending, as defined below, and/or if it meets any waiver requirements.

---

[3] (U//~~FOUO~~) In the event that a threat is identified in a 2nd Party report, the identifying target office should follow the procedures for warning/waiving in accordance with 2nd Party post-publication procedures.

[4] (U//~~FOUO~~) In the event that a threat is identified by a customer, the organization that originated the report must still follow the subsequent procedures for assessing the threat and determining whether or not it meets the requirements for a warning or a waiver. If a warning was already issued, the originating organization should reference the previous warning in their response. If a threat that meets the criteria for warning was not yet warned, the organization should approve appropriate warning language and assess why the threat was not properly identified, proactively warned by NSA. If a customer identifies a threat that requires a waiver, the organization should deny the formal request and document the target office-level waiver approval as detailed in this SOP.

Specific – information provided identifies or **suggests a potential target, period or area to be attacked**. This may require more than one piece of information to make the determination.

Credible – the information **could be accurate in general terms**. Attacker capability, the target exists, elements of the report are true, etc.

Impending – **will likely happen** at some point in the future. This could be hours, days, weeks, or months

(U) Make Determination to Warn or Request Waiver

- (U//~~FOUO~~) Based on assessment of threat, the appropriate target office designee[5] shall make determination to issue a warning or approve a waiver requests.
    - (U//~~FOUO~~) The target office will consult with key stakeholders, including IIA Ops, the NSOC SOO, and the Collection Exploitation and Cryptanalysis Operations (CECO) Directorate [redacted] as needed, in order to make the waiver determination.
    - (U//~~FOUO~~) The NSOC Senior Operations Officer (SOO) will make this determination for time-sensitive situations/after hours, in consultation with the appropriate target office, the Directorate of Operations, Operations Manager (DOOM) and/or the Counterterrorism Operations Cell Leader (NSOCCTLDR).

[redacted] (b)(3)-P.L. 86-36

(U) Issue Warning or Waiver

(U//~~FOUO~~) When the determination is made that a warning should be issued, the following steps should be followed:

- (U//~~FOUO~~) **Submit Formal Request**: The originating USSS office will submit a pro-active Post-Publication release request against the report containing the threat.
    - Go to: [redacted]
    - Select the appropriate Task Type (ORCON, NON-ORCON, FORREL, IDENT) from the menu based on the classification of the original report, the end recipient, and/or the inclusion of unmasked identities.
        - For example:
            - NON-ORCON – A warning derived from a non-ORCON report for a recipient whose country is part of the original releasability marking;

[5] Office-level management or operations staff is required to approve all waivers; however, the determination to warn can be made at lower levels, as appropriate.

- ORCON – A warning derived from a ORCON report for a recipient whose country is part of the original releasability marking;
- FORREL – A warning derived from any report for a recipient whose country is NOT part of the original releasability marking;
- IDENT – A warning that includes the unmasked identity of a U.S. or 2nd Party individual, which was masked in the original report.

o Complete form in accordance with requested information.

- **Email Address:** At a minimum you should include your email or your office alias, your office's Ops team, your office's post-pub team, your office's NSOC desk, [redacted] and the appropriate NSA/CSS liaison element [redacted]

(b)(3)-P.L. 86-36

- **Justification:** Detail the purpose for sharing this information with the intended recipient. A sample justification is provided below:

  - *(Appropriate Classification) This is a pro-active Duty to Warn (DTW) release to (Name of Potential Victim/s) based on (Report Serial). We believe that (Name of Potential Victim/s) is in imminent danger. We request that this information be relayed to the intended recipient as soon as possible to allow them time to take appropriate precautions.*

- **Handling Precedence:** If the threat is imminent, submit the request with URGENT precedence. If not imminent, submit the request with Immediate or Priority Precedence.

  - ***URGENT*** - Imminent, Identifiable Threat. Final recipient needs to take immediate, operational action (e.g. military operation, arrest).

- **Release Classification:** The classification of the request will vary, but will often be UNCLASSIFIED. The requestor should determine the appropriate classification to ensure that the intended recipient is able to receive the warning at the chosen classification, but it is not unnecessarily sanitized, if the recipient is authorized for SECRET or TS//SI reporting.

- **Proposed Sanitization:** Complete the proposed text field in accordance with the following format:

Please pass this to CIA (if threat is outside of US) or FBI (if threat is in US) with the text to be released:

~~SECRET//NOFORN~~

(Appropriate Classification) This is a pro-active Duty to Warn (DTW) release to (Name of Potential Victim/s) based on (Report Serial). We believe that (Name of Potential Victim/s) is in imminent danger. We request that this information be related to the intended recipient as soon as possible to allow them time to take appropriate precautions.

(U//~~FOUO~~) Per ICD 191, NSA is required to document and maintain records on specified duty to warn actions, one of them being how and when threat information was delivered to the intended victim. We kindly request notification of your Agency's actions within 5 business days from the date of notification for this purpose.

==========

Text to Be Released:
(Appropriate Classification) Your warning language goes here. *If the language is UNCLASSIFIED, it will need to be approved by Office-Level Chief of Ops, Deputy Chief of Ops, Chief or D/Chief.

==========

- (U//~~FOUO~~) If immediate action is needed during normal business hours, the Information Sharing and Collaboration [redacted] will assign the request through established post-publication procedures and include the NSOC Threat Warning alias [redacted] on all duty-to-warn email communications.

(b)(3)-P.L. 86-36

- (U//~~FOUO~~) If immediate action is needed after business hours, the NSOC Senior Reporting Officer (SRO) will process the request. NSOC should reach out to appropriate target office designee for advice/concurrence before any release after business hours.

- (U//~~FOUO~~) **Post-Publication Review**: The Post-Pub request is formally reviewed in accordance with standard procedures, which includes a CECO, 2nd Party, or 3rd Party equity review, as appropriate, in accordance with standard post-pub processes.

- (U//~~FOUO~~) **Provide Release Language to Customer**:

  - (U//~~FOUO~~) [redacted]/SRO provides the approved release language to the designated customer, who will be responsible in providing the warning.
  - (U//~~FOUO~~) [redacted]/SRO will inform the customer that when approved language is released, the customer(s) has five business days to provide feedback on language use.

  - (U//~~FOUO~~) ***NOTE:*** As soon as a decision to issue a warning is reached, the target office should begin coordinating with the element that will issue the warning to inform them that a duty to warn notification is in progress.

    - If the intended victim is located in the United States, the USSS analyst, Ops element, or next level supervisor will inform the FBI via the 24-hour

watch listed below, through the NSA/CSS Representative (NCR) FBI if appropriate, that a duty-to-warn notification is in progress.

- (U//~~FOUO~~) If the intended victim is located outside of the United States, the USSS analyst, Ops element, or next level supervisor will inform the DNIR/COS, through the Cryptologic Services Group (CSG) CIA, and, if appropriate, [redacted] that duty-to-warn notification is in progress.

(U//~~FOUO~~) When the determination is made that a waiver should be approved, the following steps should be followed:

- (U//~~FOUO~~) The requester of the waiver should contact and/or send an email to their office's approval authority requesting that a Duty to Warn waiver be approved. The email subject line should read, "Action: DTW Waiver Request – (very brief threat title)."
- (U//~~FOUO~~) The body of the email should include a statement requesting the waiver with an appropriate justification (see above), a brief description of the threat and information on which the threat is based with a link to, or copy of, the report in which the threat is documented.
- (U//~~FOUO~~) The Office-level waiver approval designee responds all to the waiver request email and adds the NSOC Threat Warning Alias [redacted] to document the waiver approval with NSOC. (*NOTE:* Waiver requests containing sensitive information should only be sent to the [redacted] alias.)

(b)(3)-P.L. 86-36

(U) Dispute Resolution

- (U//~~FOUO~~) If there is a dispute among internal USSS elements, resolution should occur with the next level managers. The Director of Operations will be the final adjudicator for internal USSS disputes during normal business hours; the NSOC SOO will be the final adjudicator after normal business hours. Disputes requiring Director of Operations or SOO adjudication, should be submitted threw the organizations chain of command with required review at the target office and IIA levels.
- (U//~~FOUO~~) If a customer office receives a denial for a duty-to-warn request or the USSS element has a duty-to-warn waiver approved and there is not a release of duty to warn information, the customer office can request a reclama (through the established Post-Publication process) or initiate the dispute resolution process themselves. The applicable USSS offices will be engaged as needed. The NCR FBI and CSG CIA offices shall be the initial POC for the customer office.
- (U//~~FOUO~~) If a customer submits a reclama to an NSA/CSS waiver, then Chief [redacted] Chief [redacted] in coordination with the NSOC SOO must assess the request to warn, the target office waiver, and decide to either uphold the waiver or proceed with a warning. If the reclama

is after hours, the NSOC SOO, in coordination with the appropriate Operations desks on the NSOC floor and call-ins when needed, makes the final decision on waiver determinations.

- (U//~~FOUO~~) If a USSS element has not received feedback from a customer office on the uses of its released duty-to-warn language and has made reasonable and documented steps to receive feedback, the USSS element can engage the appropriate NSA/CSS liaison office (NCR FBI or CSG CIA) to enact the ODNI-sponsored Dispute Resolution Process.

- (U//~~FOUO~~) If a USSS element is concerned about a customer's use of SIGINT information without prior consultation or notification when citing imminent threat as identified in ICD 191, Section F, paragraph 12, the USSS element should engage the appropriate NSA/CSS liaison office (NCR FBI or CSG CIA). If the issue cannot be resolved, either party may initiate the ODNI-sponsored Dispute Resolution Process outlined in ICD 191.

(U) Feedback

- (U//~~FOUO~~) IC elements that receive threat information from NSA/CSS for the purpose of delivering the information to an intended victim shall document the steps taken to deliver the threat information to the intended victim and notify NSA/CSS of the steps taken and the results. Feedback should be sent to [redacted]

Contact Information

(U//~~FOUO~~) **FBI:**

FBI CT Watch:
534-1463
[redacted]

FBI Strategic Information & Operations Center: (b)(3)-P.L. 86-36
534-1463
[redacted]

NCR FBI Contact Information:
[redacted]
717-7116 or 931-6966 (secure)
[redacted]

The NCR FBI Personnel Roster [redacted] identifies appropriate points of contact (POCs).

(U//~~FOUO~~) **CSG CIA:**

[redacted]
935-0209 (secure)
[redacted] (unclassified)

(U//~~FOUO~~) [redacted]
[redacted]

(U//~~FOUO~~) **NSOC:**

SOO: [redacted]
963-3777 (secure)
[redacted] (unclassified)

DOOM: [redacted]
963-3069 (secure)
[redacted] (unclassified)

CT-LDR: [redacted]
966-6073 (secure)

SRO: [redacted]
963-3278 (secure)

(U//~~FOUO~~) **SUSLO Offices:**

SUSLO-London:
995-7201(secure)
[redacted] (unclassified)
Contact NSOC for afterhours support

SUSLO-Canberra:
263-2100 (secure)
Contact NSOC for afterhours support

SUSLO-Ottawa:
262-2034 (secure)
[redacted] (unclassified)
Contact NSOC for afterhours support

SUSLO-Wellington:
717-8639/8638 (secure)
Contact NSOC for afterhours support

(b)(3)-P.L. 86-36

Definitions

- (U) ***Duty to Warn*** – A requirement to warn U.S. and non-U.S. persons of impending threats of intentional killing, serious bodily injury, or kidnapping.

- (U//~~FOUO~~) ***Intended Victim*** – A person or group of people, including both U.S. persons (as defined in Reference c) and non-U.S. persons, and targets that are an institution, place of business, structure, location, or electronic infrastructure that supports life.

- (U) ***Intentional Killing*** – The deliberate killing of a specific individual or group of individuals.

- (U) ***Kidnapping*** – The intentional taking of an individual or group through force or threat of force.

- (U) ***Serious Bodily Injury*** - Injury that creates a substantial risk of death or which causes serious, permanent disfigurement or impairment.